(12) UK Patent Application (19) GB (11) 2 368 951 (13) A

(43) Date of A Publication 15.05.2002

(21) Application No 0030528.4

(22) Date of Filing 14.12.2000

(30) Priority Data
(31) 0027291 (32) 08.11.2000 (33) GB

(51) INT CL[7]
G07C 9/00 , G07F 7/10

(52) UK CL (Edition T)
G4H HTG H1A H13D H14A H14D
U1S S2215

(56) Documents Cited
EP 0745961 A2
EP 0708547 A2
EP 0501697 A2
US 6125349 A
US 5764789 A

(58) Field of Search
UK CL (Edition S) G4H HTG
INT CL[7] G07C , G07F
Online: WPI, EPODOC, PAJ

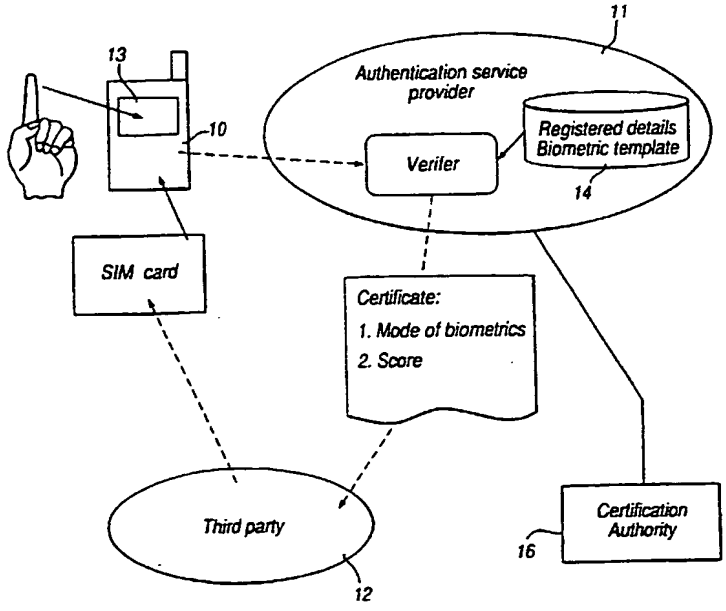
(71) Applicant(s)
Vodafone Limited
(Incorporated in the United Kingdom)
The Courtyard, 2-4 London Road, NEWBURY,
Berkshire, RG14 1JX, United Kingdom

(72) Inventor(s)
Louis Christodoulides
Nicholas Bone
Pubudu Priyanjaya Chandrasiri

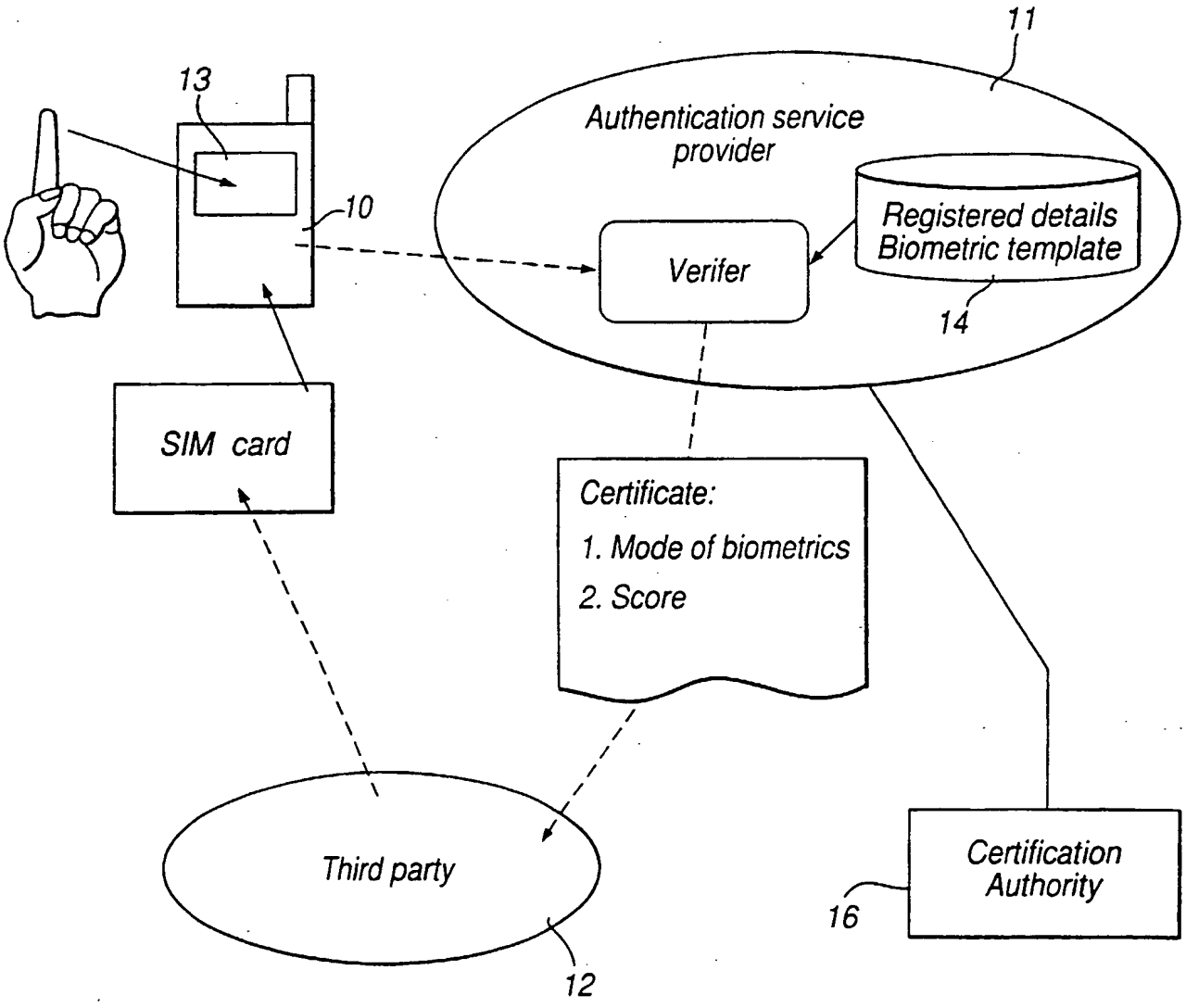
(74) Agent and/or Address for Service
Mathisen Macara & Co
The Coach House, 6-8 Swakeleys Road, Ickenham,
UXBRIDGE, Middlesex, UB10 8BZ, United Kingdom

(54) Abstract Title
User authentication

(57) An authentication system requires a user of e.g. a mobile telephone (10) to generate a signal e.g. a biometric measurement of a physical characteristic of the user e.g. fingerprint. This biometric measurement is transmitted, possibly as part of a digitally signed and encrypted message, to a remote service provider (11) where the biometric measurement is compared with a biometric template measurement of the same physical characteristic, stored for the person. The verification process produces an output which identifies the characteristic from which the biometric measurement was taken and which also gives the results of the comparison (e.g. score). A third party (12) receives this information, possibly as part of a digital certificate, and either authenticates the person or not, depending on the information. This could be used for remote transactions between the user and the third party (12).



GB 2 368 951 A



AUTHENTICATION METHODS AND SYSTEMS

The invention relates to authentication methods and systems.

Authentication may be used to check the identification of a user by means of a unique identification parameter associated with the user. Examples of such parameters are physical (biometric) characteristics such as fingerprints, a photographic facial image, an iris scan, or voice print, behavioural characteristics such as a signature, a facial expression or a body movement, and artificially created parameters such as a PIN. A user identification parameter of this kind can be measured (in the case of a biometric or behavioural characteristic) or generated (in the case of an artificially created parameter such as a PIN) and then compared with a stored template or reference parameter for that user. Particularly in cases where a biometric or behavioural characteristic is involved, such a comparison or verification process may not produce an exact correlation between the user identification parameter and the stored reference parameter. Verification algorithms are known, involving, for example, statistical spread, that allow the probability that the measured parameter emanates from the same user as the template or reference parameter to be assessed as a "score".

If, following the verification process, it is decided that the user is authenticated as "genuine", this decision can be used to permit the occurrence of some future operation. For example, it may allow a door to be opened or it may allow a commercial transaction involving that user to take place.

In many cases, the generation of the user identification parameter, its comparison with the stored reference parameter, the user authentication, and the allowance of the subsequent action, all occur at the same location. However, this need not be the case: there may be instances where the user is remote from the location where

authentication is required. In that case, it may be a problem to provide at the remote location both the means for generating the user identification parameter and the means for comparing this parameter with the stored reference parameter. An example of this problem is where the user wishes to provide the user identification parameter from a mobile telephone.

According to the invention, there is provided a method of providing authentication in response to an authentication request by a user, comprising the steps of generating a user identification parameter at an originating station in response to an input by the user, generating an identifier at the originating station, securely transmitting the user identification parameter and the identifier to an intermediate station, using the identifier received at the intermediate station to access a particular one of a plurality of stored reference identification parameters at the intermediate station, comparing the particular reference parameter at the intermediate station with the user identification parameter received there to produce an output having a value dependent on the comparison, transmitting the output to a receiving station, and making an authentication decision whether the user corresponds to the identifier in dependence on the value of the output.

According to the invention, there is further provided a method of providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where the user is one of a plurality of users known to a service provider, in which the user generates a user identification parameter, the service provider compares the user identification parameter with a particular one of a plurality of reference parameters which it stores for the plurality of users to produce an output having a value dependent on the comparison, the service provider obtains from a Certification Authority a digital certificate for the said transaction, and the service provider transmits the said output with the digital

certificate to the third party which decides whether to comply with the user's authentication request.

By separating the comparison or verification process from the generation of the user identification parameter, the originating station can be kept small and lightweight. The originating station may, for example, be a mobile device such as a mobile telephone or a personal digital assistant (PDA) or a laptop computer. Furthermore, because at least part of the verification process is separated from the originating station, there is less risk that the system will be compromised by theft or misuse of the originating station.

Authentication methods and systems according to the invention will now be described, by way of example only, with reference to the accompanying drawing the sole Figure of which is a block diagram of the system.

The system includes a mobile telephone 10 at which is generated the user identification parameter in a manner to be explained in more detail and which forms an originating station, a service provider 11 for carrying out the verification process, again in a manner to be explained in detail, and which forms an intermediate station, and a third party 12 where final authentication takes place and which forms a receiving station.

The mobile telephone 10 includes a device 13 for measuring a user identification parameter such as by making a biometric measurement of a physical characteristic of the person. As illustrated in the Figure, the identification parameter is a fingerprint but it could be any other biometric or behavioural characteristic such as any of the examples given above. It could alternatively be an artificially generated parameter such as a PIN. The mobile telephone 10 need not itself make the

measurement or generate the identification parameter; instead, it could simply receive the identification parameter from a dedicated device such as a reader.

The service provider 11 includes a database 14 which stores details of users associated with or subscribing to the service provider 11 together with a template or reference parameter for each user. The service provider 11 also includes a verifier 15 which is able to compare the identification parameter received from the mobile telephone 10 for a particular user with the reference identification parameter obtained for the same user from the database 14 and produced an output which indicates the degree of correlation ("score") between the identification parameter and the reference parameter. This output may also specify which type of identification parameter was used for the verification process.

The third party 12 receives the output from the service provider 11 and decides from this output, and from the value of the score in particular, whether the user who produced the identification parameter is the same user whose details are held by the service provider 11. There are three possible outcomes to this authentication process. The third party 12 may decide that the user is genuine, that the user is not genuine, or that the output from the service provider does not enable either determination to be made. The third party 12 produces a reply based on the authentication process as described in more detail below, which is transmitted to the mobile telephone 10. If the user is authenticated as genuine, the third party may then agree that some specific action takes place such as a financial transaction.

An example of the use of the system will now be described in relation to a desired purchase by a user of goods offered for sale by the third party 12.

When the user indicates a wish to enter into a transaction with the third party 12, the third party 12 requests authentication. On receiving this request, the user, in the system illustrated in the Figure, applies their finger to the device 13 on the mobile telephone 10 to produce a digital signal representing (in this example) a biometric measurement of the fingerprint, that is, the user identification parameter.

The service provider 11 can only carry out the verification process if it knows the purported identity of the user – because it must download the appropriate reference parameter from its database 14 in order to carry out the verification process; that is, the verification process involves a one-to-one comparison of an identification parameter and a reference parameter, and not a one-to-many comparison which would involve comparing the identification parameter with all the stored reference parameters. In other words, therefore, the user must provide some signal (an identifier) to the service provider which indicates the identity (or at least the purported identity) of the user and enables the service provider to download the appropriate reference parameter from the database. The identifier does not have to identify the user by name. For example, the signal identifier could be a password or could comprise the CLI (Calling Line Identifier) of the mobile telephone.

In this way, therefore, the mobile telephone 10 may generate a digitally signed message which (a) indicates the identity or the purported identity of the user, or of the mobile telephone and (b) incorporates the digital signal representing the user identification parameter. This message is encrypted and transmitted from the mobile telephone 10 to the service provider.

It is important that the message from the mobile telephone 10 to the service provider 11 is sent in a secure way. If the message could be intercepted in a way which permitted an unauthorised person to come into possession of the user's

identification parameter, the user's security would be compromised. Although, in principle, a biometric or behavioural identification parameter gives greater security than an artificially generated one such as a PIN, an artificially generated parameter can be changed if compromised, whereas this is not possible, or not easily possible, in the case of a biometric or behavioural identification parameter.

The message from the mobile telephone 10 to the service provider 11 will also include a transaction message which will indicate the nature of the transaction which the user wishes to carry out with the third party. This message is also encrypted.

In a modification, a mobile telephone is not used to transmit the user's identification parameter (and the transaction message) to the service provider. For example, a suitable terminal (e.g. in a retail outlet) may be provided which measures or generates the user's identification parameter and then transmits it, together with the user identifier (e.g. a PIN input into the terminal by the user) to the service provider. The message could in such a case be transmitted along a hard-wired connection such as a fixed PSTN connection, in which case unauthorised interception is much more difficult and the need for encryption of the message is less or absent.

In response to receipt of the digitally signed message from the mobile telephone 10, the verifier 15 in the service provider 11 uses the identifier identifying the user or the user's telephone to download the reference parameter for that user from the database 14. The verifier then performs a comparison between the identification parameter received via the mobile telephone with this reference parameter, in order to produce an output indicating the degree of correlation between the compared parameters (the "score").

If the score is very low, the service provider 11 may then simply send a signal back to the mobile telephone 10 asking the user to carry out another measurement of the user identification parameter and to repeat the process, or the service provider may simply reject the user completely.

In a general case, though, the service provider incorporates the score into a message which is then transmitted to the third party 12. The message will not only include the score but other information concerning the verification process and the user. For example, the message can signify the particular type of biometric or other measurement used in the verification process, and may include such user information as (for example) the credit-worthiness of the user or the user's remaining credit amount) which the service provider 11 would store in its database 14. Details of the transaction (that is, from the transaction message sent by the requesting user) will also be included.

The message transmitted from the service provider 11 to the third party 12 can be transmitted in any suitably secure way which enables the third party 12 to satisfy itself that the message does indeed emanate from the service provider 11. For example, it could be incorporated into a digital certificate produced for that purpose (e.g. the message could be incorporated as an extension to the certificate). However, instead it could be sent via an encrypted and authenticated channel or by a fixed tamper-proof connection.

On receiving the message from the service provider, the third party makes a determination, on the basis of the "score" received from the service provider, whether to regard the user as "genuine". If it determines that the user is genuine, it may then consider other data (e.g. the data received from the service provider concerning the user's credit worthiness) before making a final decision whether to permit the proposed transaction. If it decides to allow the transaction, it will then

signal this back to the mobile telephone 10 via the service provider 11. Instead, though, it may (as described above) reject the transaction completely or perhaps make a conditional rejection: it might permit part of the transaction (e.g. up to a reduced financial limit) or it might ask for the identification process to be repeated.

In principle, and as described, the system separates verification (carried out by the service provider 11) and authentication carried out by the third party 12. However, the service provider 11 may itself carry out a "pre-authentication" process. For example, the service provider may be concerned about responsibility which it may have for any transaction message passed to the third party, particularly if this is a digitally signed message, and the service provider has already issued a long-lived certificate associating the signing key with a legitimate user. In such a case, therefore, it may wish to reserve the right to block the transmission of the transaction message unless it is reasonably convinced that the user is genuine. Thus, the service provider's pre-authentication process could require a lower level of certainty (of the user's genuineness), that is, a lower score, than the final authentication process carried out by the third party.

The system describes allows verification to take place remotely from the mobile telephone or other originating station. The originating station simply requires a device that can take the physical measurement necessary to produce the identification parameter. The service provider is well placed to carry out the verification process because it will normally store details of its subscribers on its database, and these details simply need to be amplified to include the relevant reference parameters for the different users. The correlation score produced by the verification process can be transmitted to the third party as part of the already pre-defined infra-structure of digital certificates and thus uses a standard format that

can be read by any normal implementation of digital certificate services, perhaps with some small modification.

As indicated earlier, an advantage of the system and method described is that the verification process is not carried out at the originating station (such as the mobile telephone 10), but is instead carried out centrally by the service provider. This reduces the amount of processing which must be carried out at the originating station and also improves security. However, in the modification, part of the verification process may be carried out at the originating station. For example, in the case where the originating station is a GSM mobile telephone employing a SIM card which has significant data processing capabilities, part of the verification process may be carried out by the SIM card. Thus, for example, the SIM card would receive the measured identification parameter from the measurement device 13 (see the Figure) and would carry out a preliminary comparison with stored data representing a simplified version of, or some function of, the reference parameter. Only if this initial verification process is satisfactorily completed (that is, the "score" exceeds a predetermined value) is the digitally signed and encrypted message, containing any intended transaction message and the user identification parameter, generated and transmitted to the service provider 11. In this case, also, the message would include the results of the preliminary verification process. The use of a preliminary verification process of this form, carried out at the originating station, serves to eliminate clearly faulty measurements of a user identification parameter, or clearly fraudulent users, at an early stage and reduces the transmission of unnecessary messages to the service provider and fraudulent transactions to the third party. Because only part of the verification process is carried out at the originating station, the security of the whole system would not be significantly compromised by (for example) theft of the mobile telephone or SIM card.

In such an arrangement, the verification process carried out at the service provider 11 can comprise such a process carried out with the remaining part, only, of the reference parameter. In this case, therefore, if the service provider's operations become compromised in some way only the part of the reference parameter which needs to be stored in the service provider's database will be compromised.

Instead, though, the complete verification process can be carried out at the service provider 11, that is, repeating the part carried out at the originating station.

In order to improve security, the service provider 11 may request a short-lived or temporary certificate from a Certification Authority (CA) shown at 16 in the Figure. The certificate issuance and expiry times are sufficiently close together so that only the particular transaction with the third party 12 which is currently being requested by the user at the originating station will be covered. The service provider obtains this short-term certification from the CA 16, attaches data representing the "score" resulting from the comparison process which it has carried out and transmits the certificate to the third party 12 which makes the final decision (acceptance or rejection) and responds accordingly in the manner explained.

The service provider 11 preferably includes (in an additional extension field of the certificate) a digest of the message from the mobile 10. This strengthens security by indicating that only one signed message can be validated by the certificate.

For further security, it is desirable that the whole transaction is time-stamped (e.g. to prevent the user attempting subsequently to resile from a transaction by denying that the mobile telephone 10 was in the user's possession at the time when the transaction was initiated. The use of the short term certificate, obtained from the CA 16 in the manner explained, provides such a time stamp. Moreover, because

the CA 16 is independent, the time stamp has independent authority (as compared with internal time-stamping generated by the service provider 11 or the third party 12). This may therefore enable the use of a separate, independent, time-stamping service to be avoided, with consequent cost serving.

The service provider could be arranged to store for each user a record of the "scores" produced for successive verifications for that user. Such a record could show a "pattern" of scores, and a sudden and substantial change in the pattern might indicate a potentially suspect user identification parameter.

The authentication need not be used for a commercial transaction, it could be used for any purpose. For example, it could be used to perform any remote function that requires authentication.

Although the above description implies a biometric or behavioural measurement, this need not be the case. Instead, the user identification parameter could be a signature or PIN, and these would of course be processed in the manner already explained.

CLAIMS

1. A method of providing authentication in response to an authentication request by a user, comprising the steps of generating a user identification parameter at an originating station in response to an input by the user, generating an identifier at the originating station, securely transmitting the user identification parameter and the identifier to an intermediate station, using the identifier received at the intermediate station to access a particular one of a plurality of stored reference identification parameters at the intermediate station, comparing the particular reference parameter at the intermediate station with the user identification parameter received there to produce an output having a value dependent on the comparison, transmitting the output to a receiving station, and making an authentication decision whether the user corresponds to the identifier in dependence on the value of the output.

2. A method according to claim 1, in which the user identification parameter is a biometric or behavioural parameter relating to the user.

3. A method according to claim 1, in which the user identification parameter is a signal generated by the user such as a PIN.

4. A method according to any preceding claim, in which the identifier is an identifier signal automatically generated at the originating station in response to the user's authentication request.

5. A method according to claim 4, in which the identifier is automatically generated by a smart card.

6. A method according to claim 4 or 5, in which the originating station is or includes a mobile telephone or telecommunications terminal unit and the identifier is generated thereby.

7. A method according to claim 6, in which the identifier is the calling line identifier of the mobile terminal.

8. A method according to claim any one of claims 1 to 3, in which the identifier is input by the user.

9. A method according to any preceding claim, including the step of carrying out a comparison at the originating station between the user identification parameter and a local reference parameter, and the step of blocking the transmission of the user identification parameter to the intermediate station unless the said comparison produces at least a predetermined degree of correlation.

10. A method according to claim 9, in which the local reference parameter is a function of the particular one of the stored reference identification parameters.

11. A method according to claim 9 or 10, in which the local reference parameter is stored on and accessed at the originating station from a smart card.

12. A method according to claim 11, in which the smart card is a SIM.

13. A method according to any preceding claim, in which the value of the output includes a score representing the degree of correlation between the user identification parameter and the stored reference parameter with which it is compared.

14. A method according to claim 13, in which the value of the output includes a record of the pattern of a plurality of the said scores corresponding to a plurality of comparisons with the same stored reference parameter .

15. A method according to claim 13 or 14, in which the output is provided to the receiving station only if the score exceeds a predetermined value.

16. A method according to claim 14, in which the output is provided to the receiving station only if the score is consistent with the said pattern.

17. A method according to any preceding claim, in which the user identification parameter is transmitted to the intermediate station in encrypted form.

18. A method according to any preceding claim, in which the output is transmitted to the receiving station in a manner which authenticates the intermediate station as the transmitter.

19. A method according to claim 18, in which the output is included in an extension to a digital certificate.

20. A method according to claim 19, in which the digital certificate has a lifetime sufficiently short to cover only a single comparison by the receiving station.

21. A method according to any preceding claim, in which the originating station is one of a plurality of originating stations, the intermediate station storing reference identification parameters for all of said plurality of originating stations.

22. A method of providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where a plurality of users are known to a service provider, in which the requesting user generates a user identification parameter, the service provider compares the user identification parameter with a particular one of a plurality of reference parameters which it stores for the plurality of known users to produce an output having a value dependent on the comparison, the service provider obtains from a Certification Authority a digital certificate for the said transaction, and the service provider transmits the said output with the digital certificate to the third party which decides whether to comply with the user's authentication request.

23. A method according to claim 22, in which the digital certificate certifies the time of the transaction.

24. A method according to claim 22 or 23, in which the digital certificate contains a digest of the transaction.

25. A method according to any one of claims 22 to 24, in which the digital certificate is a temporary certificate having a lifetime only sufficient for the said transaction.

26. A method according to any one of claims 22 to 25, in which the user identification parameter is generated by the requesting user at an originating station and transmitted to the service provider in a manner resistive to interception.

27. A method according to claim 26, in which the user identification parameter is transmitted to the service provider in encrypted form.

28. A method according to any one of claims 22 to 27, in which the user generates a transaction message for the third party which is first transmitted to the service provider in encrypted form.

29. A method according to claim 28, in which the transaction message is blocked by the service provider if the service provider is not satisfied that the requesting user is one of the known users.

30. A method according to any one of claims 26 to 29, in which the originating station is or includes a mobile telephone or telecommunications terminal.

31. A method according to any one of claims 22 to 30, in which the originating station transmits an identifier to the service provider which uses the identifier to access the particular one of the stored reference parameters.

32. A method according to any one of claims 22 to 31, in which the user identification parameter is a biometric or behavioural parameter obtained from the requesting user.

33. Apparatus for providing authentication in response to an authentication request by a user, comprising identification means for generating a user identification parameter at an originating station in response to an input by the user, means for generating an identifier at the originating station, transmitting means for securely transmitting the user identification parameter and the identifier to an intermediate station, means at the intermediate station responsive to the identifier received for accessing a particular one of a plurality of stored reference identification parameters at the intermediate station, comparing means for comparing the particular reference parameter at the intermediate station with the user identification parameter received there to produce an output having a value

dependent on the comparison, means for transmitting the output to a receiving station, means for making an authentication decision whether the user corresponds to the identifier in dependence on the value of the output.

34. Apparatus according to claim 33, in which the user identification parameter is a biometric or behavioural parameter relating to the user.

35. Apparatus according to claim 33, in which the user identification parameter is a signal generated by the user such as a PIN.

36. Apparatus according to any one of claims 33 to 35, in which the identifier is an identifier signal automatically generated at the originating station in response to the user's authentication request.

37. Apparatus according to claim 36, in which the identifier signal is automatically generated by a smart card.

38. Apparatus according to claim 36 or 37, in which the originating station is or includes a mobile telephone or telecommunications terminal unit and the identifier is generated thereby.

39. Apparatus according to claim 38, in which the identifier is the calling line identifier of the mobile terminal.

40. Apparatus according to any one of claims 33 to 35, in which the identifier signal is input by the user.

41. Apparatus according to any one of claims 33 to 39, including means at the originating station for carrying out a comparison between the user identification

parameter and a local reference parameter, and means for blocking the transmission of the user identification parameter to the intermediate station unless the said comparison produces at least a predetermined degree of correlation.

42. Apparatus according to claim 41, in which the local reference parameter is a function of the particular one of the stored reference identification parameters.

43. Apparatus according to claim 41 or 42, in which the local reference parameter is stored on and accessed at the originating station from a smart card.

44. Apparatus according to claim 43, in which the smart card is a SIM.

45. Apparatus according to any one of claims 30 to 41, in which the value of the output includes a score representing the degree of correlation between the user identification parameter and the stored reference parameter with which it is compared.

46. Apparatus according to claim 45, in which the value of the output includes a record of the pattern of a plurality of the said scores corresponding to a plurality of comparisons with the same stored reference parameter.

47. Apparatus according to claim 45 or 46, in which the output is provided to the receiving station only if the score exceeds a predetermined value.

48. Apparatus according to claim 46, in which the output is provided to the receiving station only if the score is consistent with the said pattern.

49. Apparatus according to any one of claims 33 to 48, including means for transmitting the user identification parameter to the intermediate station in encrypted form.

50. Apparatus according to any one of claims 33 to 49, in which the output is transmitted to the receiving station in a manner which authenticates the intermediate station as the transmitter.

51. Apparatus according to claim 50, in which the output is included in an extension to a digital certificate.

52. Apparatus according to claim 51, in which the digital certificate has a lifetime sufficiently short to cover only a single comparison by the receiving station.

53. Apparatus according to any one of claims 33 to 52, in which the originating station is one of a plurality of originating stations, the intermediate station storing reference identification parameters for all of said plurality of originating stations.

54. Apparatus for providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where a plurality of users are known to a service provider, including means responsive to the requesting user for generating a user identification parameter, means at the service provider for comparing the user identification , in which the output is provided to the receiving station only if the score exceeds a predetermined value.

48. Apparatus according to claim 46, in which the output is provided to the receiving station only if the score is consistent with the said pattern.

49. Apparatus according to any one of claims 33 to 48, including means for transmitting the user identification parameter to the intermediate station in encrypted form.

50. Apparatus according to any one of claims 33 to 49, in which the output is transmitted to the receiving station in a manner which authenticates the intermediate station as the transmitter.

51. Apparatus according to claim 50, in which the output is included in an extension to a digital certificate.

52. Apparatus according to claim 51, in which the digital certificate has a lifetime sufficiently short to cover only a single comparison by the receiving station.

53. Apparatus according to any one of claims 33 to 52, in which the originating station is one of a plurality of originating stations, the intermediate station storing reference identification parameters for all of said plurality of originating stations.

54. Apparatus for providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where a plurality of users are known to a service provider, including means responsive to the requesting user for generating a user identification parameter, means at the service provider for comparing the user identification parameter with a particular one of a plurality of reference parameters which it stores for the plurality of known users to produce an output having a value dependent on the comparison, means at the service provider for obtaining from a Certification Authority a digital certificate for the said transaction, transmitting means for transmitting the said output with

the digital certificate from the service provider to the third party which decides whether to comply with the user's authentication request.

55. Apparatus according to claim 54, in which the digital certificate certifies the time of the transaction.

56. Apparatus according to claim 54 or 55, in which the digital certificate contains a digest of the transaction.

57. Apparatus according to any one of claims 54 to 56, in which the digital certificate is a temporary certificate having a lifetime only sufficient for the said transaction.

58. Apparatus according to any one of claims 54 to 57, in which the user identification parameter is generated by requesting user at an originating station and transmitted to the service provider in a manner resistive to interception.

59. Apparatus according to claim 58, in which the user identification parameter is transmitted to the service provider in encrypted form.

60. Apparatus according to any one of claims 54 to 59, in which the user generates a transaction message for the third party which is first transmitted to the service provider in encrypted form.

61. Apparatus according to claim 60, including means at the service provider for blocking the transaction message if the service provider is not satisfied that the requesting user is one of the known users.

62. A method of providing authentication in response to an authentication request by a user, substantially as described with reference to the accompanying drawing.

63. Apparatus for providing authentication in response to an authentication request by a user, substantially as described with reference to the accompanying drawing.

Amendments to the claims have been filed as follows

CLAIMS

1. A method of providing authentication in response to an authentication request by a user, comprising the steps of generating a user identification parameter at an originating station in response to an input by the user, generating an identifier at the originating station, securely transmitting the user identification parameter and the identifier to an intermediate station, using the identifier received at the intermediate station to access a particular one of a plurality of stored reference identification parameters at the intermediate station, comparing the particular reference parameter at the intermediate station with the user identification parameter received there to produce an output having a value dependent on the comparison, transmitting the output to a receiving station, and making an authentication decision whether the user corresponds to the identifier in dependence on the value of the output.

2. A method according to claim 1, in which the user identification parameter is a biometric or behavioural parameter relating to the user.

3. A method according to claim 1, in which the user identification parameter is a signal generated by the user such as a PIN.

4. A method according to any preceding claim, in which the identifier is an identifier signal automatically generated at the originating station in response to the user's authentication request.

5. A method according to claim 4, in which the identifier is automatically generated by a smart card.

6. A method according to claim 4 or 5, in which the originating station is or includes a mobile telephone or telecommunications terminal unit and the identifier is generated thereby.

7. A method according to claim 6, in which the identifier is the calling line identifier of the mobile terminal.

8. A method according to claim any one of claims 1 to 3, in which the identifier is input by the user.

9. A method according to any preceding claim, including the step of carrying out a comparison at the originating station between the user identification parameter and a local reference parameter, and the step of blocking the transmission of the user identification parameter to the intermediate station unless the said comparison produces at least a predetermined degree of correlation.

10. A method according to claim 9, in which the local reference parameter is a function of the particular one of the stored reference identification parameters.

11. A method according to claim 9 or 10, in which the local reference parameter is stored on and accessed at the originating station from a smart card.

12. A method according to claim 11, in which the smart card is a SIM.

13. A method according to any preceding claim, in which the value of the output includes a score representing the degree of correlation between the user identification parameter and the stored reference parameter with which it is compared.

14. A method according to claim 13, in which the value of the output includes a record of the pattern of a plurality of the said scores corresponding to a plurality of comparisons with the same stored reference parameter .

15. A method according to claim 13 or 14, in which the output is provided to the receiving station only if the score exceeds a predetermined value.

16. A method according to claim 14, in which the output is provided to the receiving station only if the score is consistent with the said pattern.

17. A method according to any preceding claim, in which the user identification parameter is transmitted to the intermediate station in encrypted form.

18. A method according to any preceding claim, in which the output is transmitted to the receiving station in a manner which authenticates the intermediate station as the transmitter.

19. A method according to claim 18, in which the output is included in an extension to a digital certificate.

20. A method according to claim 19, in which the digital certificate has a lifetime sufficiently short to cover only a single comparison by the receiving station.

21. A method according to any preceding claim, in which the originating station is one of a plurality of originating stations, the intermediate station storing reference identification parameters for all of said plurality of originating stations.

22. A method of providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where a plurality of users are known to a service provider, in which the requesting user generates a user identification parameter, the service provider compares the user identification parameter with a particular one of a plurality of reference parameters which it stores for the plurality of known users to produce an output having a value dependent on the comparison, the service provider obtains from a Certification Authority a digital certificate for the said transaction, and the service provider transmits the said output with the digital certificate to the third party which decides whether to comply with the user's authentication request.

23. A method according to claim 22, in which the digital certificate certifies the time of the transaction.

24. A method according to claim 22 or 23, in which the digital certificate contains a digest of the transaction.

25. A method according to any one of claims 22 to 24, in which the digital certificate is a temporary certificate having a lifetime only sufficient for the said transaction.

26. A method according to any one of claims 22 to 25, in which the user identification parameter is generated by the requesting user at an originating station and transmitted to the service provider in a manner resistive to interception.

27. A method according to claim 26, in which the user identification parameter is transmitted to the service provider in encrypted form.

28. A method according to any one of claims 22 to 27, in which the user generates a transaction message for the third party which is first transmitted to the service provider in encrypted form.

29. A method according to claim 28, in which the transaction message is blocked by the service provider if the service provider is not satisfied that the requesting user is one of the known users.

30. A method according to any one of claims 26 to 29, in which the originating station is or includes a mobile telephone or telecommunications terminal.

31. A method according to any one of claims 22 to 30, in which the originating station transmits an identifier to the service provider which uses the identifier to access the particular one of the stored reference parameters.

32. A method according to any one of claims 22 to 31, in which the user identification parameter is a biometric or behavioural parameter obtained from the requesting user.

33. Apparatus for providing authentication in response to an authentication request by a user, comprising identification means for generating a user identification parameter at an originating station in response to an input by the user, means for generating an identifier at the originating station, transmitting means for securely transmitting the user identification parameter and the identifier to an intermediate station, means at the intermediate station responsive to the identifier received for accessing a particular one of a plurality of stored reference identification parameters at the intermediate station, comparing means for comparing the particular reference parameter at the intermediate station with the user identification parameter received there to produce an output having a value

dependent on the comparison, means for transmitting the output to a receiving station, means for making an authentication decision whether the user corresponds to the identifier in dependence on the value of the output.

34. Apparatus according to claim 33, in which the user identification parameter is a biometric or behavioural parameter relating to the user.

35. Apparatus according to claim 33, in which the user identification parameter is a signal generated by the user such as a PIN.

36. Apparatus according to any one of claims 33 to 35, in which the identifier is an identifier signal automatically generated at the originating station in response to the user's authentication request.

37. Apparatus according to claim 36, in which the identifier signal is automatically generated by a smart card.

38. Apparatus according to claim 36 or 37, in which the originating station is or includes a mobile telephone or telecommunications terminal unit and the identifier is generated thereby.

39. Apparatus according to claim 38, in which the identifier is the calling line identifier of the mobile terminal.

40. Apparatus according to any one of claims 33 to 35, in which the identifier signal is input by the user.

41. Apparatus according to any one of claims 33 to 39, including means at the originating station for carrying out a comparison between the user identification

parameter and a local reference parameter, and means for blocking the transmission of the user identification parameter to the intermediate station unless the said comparison produces at least a predetermined degree of correlation.

42. Apparatus according to claim 41, in which the local reference parameter is a function of the particular one of the stored reference identification parameters.

43. Apparatus according to claim 41 or 42, in which the local reference parameter is stored on and accessed at the originating station from a smart card.

44. Apparatus according to claim 43, in which the smart card is a SIM.

45. Apparatus according to any one of claims 30 to 41, in which the value of the output includes a score representing the degree of correlation between the user identification parameter and the stored reference parameter with which it is compared.

46. Apparatus according to claim 45, in which the value of the output includes a record of the pattern of a plurality of the said scores corresponding to a plurality of comparisons with the same stored reference parameter.

47. Apparatus according to claim 45 or 46, in which the output is provided to the receiving station only if the score exceeds a predetermined value.

48. Apparatus according to claim 46, in which the output is provided to the receiving station only if the score is consistent with the said pattern.

49. Apparatus according to any one of claims 33 to 48, including means for transmitting the user identification parameter to the intermediate station in encrypted form.

50. Apparatus according to any one of claims 33 to 49, in which the output is transmitted to the receiving station in a manner which authenticates the intermediate station as the transmitter.

51. Apparatus according to claim 50, in which the output is included in an extension to a digital certificate.

52. Apparatus according to claim 51, in which the digital certificate has a lifetime sufficiently short to cover only a single comparison by the receiving station.

53. Apparatus according to any one of claims 33 to 52, in which the originating station is one of a plurality of originating stations, the intermediate station storing reference identification parameters for all of said plurality of originating stations.

54. Apparatus for providing authentication in response to an authentication request by a user wishing to make a transaction with a third party where a plurality of users are known to a service provider, including means responsive to the requesting user for generating a user identification parameter, means at the service provider for comparing

the user identification parameter with a particular one of a plurality of reference parameters which it stores for the plurality of known users to produce an output having a value dependent on the comparison, means at the service provider for obtaining from a Certification Authority a digital certificate for the said transaction, and transmitting means for transmitting the said output with the digital certificate from the service provider to the third party which decides whether to comply with the user's authentication request.

55. Apparatus according to claim 54, in which the digital certificate certifies the time of the transaction.

56. Apparatus according to claim 54 or 55, in which the digital certificate contains a digest of the transaction.

57. Apparatus according to any one of claims 54 to 56, in which the digital certificate is a temporary certificate having a lifetime only sufficient for the said transaction.

58. Apparatus according to any one of claims 54 to 57, in which the user identification parameter is generated by the requesting user at an originating station and transmitted to the service provider in a manner resistive to interception.

59. Apparatus according to claim 58, in which the user identification parameter is transmitted to the service provider in encrypted form.

60. Apparatus according to any one of claims 54 to 59, in which the user generates a transaction message for the third party which is first transmitted to the service provider in encrypted form.

61. Apparatus according to claim 60, including means at the service provider for blocking the transaction message if the service provider is not satisfied that the requesting user is one of the known users.

62. A method of providing authentication in response to an authentication request by a user, substantially as described with reference to the accompanying drawing.

63. Apparatus for providing authentication in response to an authentication request by a user, substantially as described with reference to the accompanying drawing.

Application No: GB 0030528.4
Claims searched: 1,33 & appendancies
Examiner: Mike Davis
Date of search: 27 February 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4H (HTG)

Int Cl (Ed.7): G07C, G07F

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0745961 A2	(AT&T)	1,33 at least
X	EP 0708547 A2	(AT&T)	"
X	EP 0501697 A2	(AT&T)	"
X	US 5764789	(PARE JR. ET AL)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB_____2368951A__I_>

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB 0030528.4
Claims searched: 22-32 & 54-61
Examiner: Melanie Gee
Date of search: 23 August 2001

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications. in:

UK Cl (Ed.S): G4H (HTG)

Int Cl (Ed.7): G07C; G07F

Other: Online: WPI, EPODOC, PAJ

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	EP 0708547 A2 (AT & T), see col. 5 line 57 - col. 6 line 41.	
A	US 6125349 A (MAHER), see col. 5 line 36 - col. 6 line 24.	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB_____2368951A__I_>